UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/977,203	10/16/2001	Marc Charbonneau	12-67 US	3581

25319 7590 06/28/2005

FREEDMAN & ASSOCIATES
117 CENTREPOINTE DRIVE
SUITE 350
NEPEAN, ONTARIO, K2G 5X3
CANADA

EXAMINER	
PARTHASARATHY, PRAMILA	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 06/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/977,203	CHARBONNEAU, MARC	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 April 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on April 12, 2005. Claims 1 and 17 have been amended. Claims 1 – 24 are pending.

Response to Remarks/Arguments

Specification

2. The disclosure is objected to because of the following informalities: US publication 2003/0074567A1, Page 4 paragraph [0039] reads, ".. As is evident tot hose...". Replace with "..As is evident to those ..".

Appropriate correction is required.

Examiner suggests that in response to this action, applicant corrects any other typographical errors that are not addressed before.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 1 – 16 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

The amended independent Claim 1 recites, " ... a trusted state of executable **programs** in execution ..." and "... a current state of executable **programs** in execution ...".

With respect to "a trusted state of executable **programs** in execution" and "a current state of executable **programs** in execution", although the instant application (Background of the invention, US2003/0074567A1, Page 1 paragraph [0007 – 0008]), discusses that U.S. Patent number 5,919,257 discloses, "a networked workstation performs an intrusion detection hashing function on selected workstation executable program(s)." and "The server can computer the trusted hash value(s) by performing the hashing function on trusted copies of the selected workstation executable programs stored in the server ...", the specification does not disclose "... a trusted state of executable **programs** in execution ..." and "... a current state of executable **programs** in execution ..." (emphasis added).

Applicant amendment does not clarify and direct wherein the specification such support is disclosed for "... a trusted state of executable programs in execution ..." and "... a current state of executable programs in execution ...".

The dependent claims 2 – 16 are rejected at least by virtue of their dependency on the dependent claims.

4. Claims 1 – 24 were rejected under 35 USC 102(e) as being anticipated by Langford et al. (U.S. Patent Number 6,470,450, hereafter "Langford") and in response, Applicant amended Claims 1 and 17.

5. Applicant's remarks/arguments filed on April 12, 2005, with respect to amended Claims 1 and 17, have been fully considered but they are not persuasive. Referring to the previous Office action, Examiner had cited relevant portions of the references as a means to illustrate the system as taught by the prior art. As a means of providing further clarification as to what is taught by the references used in the first office action, Examiner has expanded the teachings for comprehensibility while maintaining the same grounds of rejection of the claims.

Langford teaches systems and methods for controlling software application access to limited access based data, wherein each application unit or computing unit generates a hash value to determine application access by comparing computed application identification data and stored unique application verification data. Furthermore, Langford teaches that the term application includes libraries, groups of applications (programs) or any suitable access mechanisms that uses (directly or indirectly) limited access based data.

6. Regarding amended independent Claims 1 and 17, Applicant agrees that Langford teaches determining a hash value of an application, checking whether a computed hash value of the executable file data matches the corresponding stored unique application verification data and stored unique application verification data relating to a requesting application, but argues that the distinction between the prior art and the instant application is that in the present invention "receiving a trusted hash value relating to predetermined data stored in memory within the computer system for a trusted state of executable **programs** (plural form) in execution within the computer system", "determining a computed hash value for a current state of executable **programs** (plural form) in execution within the computer system" and "wherein the predetermined data relates to programs in execution on the computer system when the computer system is in a known secure state". These arguments are not persuasive.

Langford discloses "receiving a trusted hash value relating to predetermined data stored in memory within the computer system for a trusted state of executable programs in execution within the computer system" (Column 3 lines 36 – 44 and Column 4 lines 15 – 30), further discloses that the hash value is generated of stored application**s** (groups application**s**) (Column 9 lines 7 – 14); "determining a computed hash value for a current state of executable programs in execution within the computer system" (Column 3 lines 5 – 30, 36 – 44 and Column 4 lines 1 – 4), further discloses that the hash value is computed for a current state of executable application**s** (program**s**) (Column 9 lines 7 – 14); and "wherein the predetermined data relates to programs in execution on the

computer system when the computer system is in a known secure state" (Column 3 lines 5 – 30, 36 – 44 and Column 4 lines 1 – 4), further discloses that the system grants the application access only when the predetermined data is related to the program in execution on the processor of the computer system when the computer system is in a known secure state (Column 7 lines 23 – 60).

7. Applicant clearly has failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts. Therefore, the examiner respectfully asserts that cited prior art does teach or suggest the subject matter broadly recited in independent claims 1 and 17. Dependent claims 2 – 16 and 18 – 24 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action.

Accordingly, the rejection for the pending Claims 1 – 24 is respectfully maintained.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1 – 24 are rejected under 35 U.S.C. 102(e) as being anticipated by Langford et al. (U.S. Patent Number 6,470,450).

Regarding Claim 1, Langford teaches and describes a method of detecting unauthorized executable programs resident in a computer system memory comprising the steps of:

receiving a trusted hash value representative of a hash value for generation by a predetermined hashing process of predetermined data stored in memory within the computer system for a trusted state of executable programs in execution within the computer system if an unauthorized executable program is other than resident in the computer system (Column 3 lines 36 – 44, Column 4 lines 15 – 30 and Column 9 lines 7 – 14);

hashing data stored in memory within the computer system using the predetermined hashing process to determine a computed hash value for a current state of executable programs in execution within the computer system (Column 3 lines 5 – 30, 36 – 44, Column 4 lines 1 – 4 and Column 9 lines 7 – 14); and

comparing the computed hash value and the trusted hash value to determine differences between the data and the predetermined data (Column 3 lines 23 – 30 and Column 4 lines 30 – 38).

Regarding Claim 17, Langford teaches and describes a method of detecting unauthorized executable programs resident in a computer system comprising the steps of:

a) providing a trusted security application executable on a processor of the computer system for determining a hash value using a predetermined hashing process of predetermined data existing in memory within the computer system (Column 3 lines 36 – 44 and Column 4 lines 15 – 30);

b) hashing the predetermined data existing in memory within the computer system using the predetermined process to determine a hash value (Column 3 lines 5 – 30, 36 – 44 and Column 4 lines 1 – 4);

c) digitally signing the hash value to provide a trusted hash value (Column 3 lines 31 – 35 and Column 4 lines 1 – 7 and 26 – 44); and

d) retrievably storing the trusted hash value, wherein the predetermined data relates to programs in execution on the processor of the computer system when the computer system is in a known secure state (Column 4 lines 1 – 7, Column 5 lines 10 – 15 and Column 7 lines 23 – 60).

Claim 2 is rejected applied as above in rejecting Claim 1. Furthermore, Langford teaches and describes a method of detecting unauthorized executable programs resident in a computer system memory including the steps of

aa) receiving user authorization information (Column 5 line 62 – Column 6 line 1);

aaa) authenticating the user authorization information to perform at least one of

authorize and identify a user (Column 5 line 62 – Column 6 line 5); and

aaaa) when the user is at least one of authorized or identified, requesting security data of the user (Column 6 line 2 – 9).

Claim 5 is rejected applied as above in rejecting Claim 1. Furthermore, Langford teaches and describes a method of detecting unauthorized executable programs resident in a computer system memory, comprising the steps of:

receiving a request for security data from an application in execution in the computer system (Column 4 lines 26 – 44 and Column 5 lines 36 – 42); and,

when the comparison is indicative of other than an unauthorized executable programs resident in a computer system, providing security data to the application (Column 6 lines 44 – 48 and Column 8 lines 49 – 53)).

Claim 6 is rejected applied as above in rejecting Claim 1. Furthermore, Langford teaches and describes a method of detecting unauthorized executable programs resident in a computer system memory, wherein

the trusted hash value and the computed hash value are determined by a same trusted security application executing locally on a processor of a same computer system at different times, the trusted hash value determined when the computer system is in a known secure state (Column 3 lines 5 – 17 and 36 – 44).

Claim 8 is rejected applied as above in rejecting Claim 1. Furthermore, Langford teaches and describes a method of detecting unauthorized executable programs resident in a computer system memory, including the step of:

b1) verifying an authenticity of the digitally signed trusted hash value (Column 5 lines 24 – 35 and Column 6 lines 30 – 41).

Claim 22 is rejected applied as above in rejecting Claim 1. Furthermore, Langford teaches and describes a method of detecting unauthorized executable programs resident in a computer system memory, wherein predetermined data includes DLL tables (Column 3 lines 19 – 30).

Claim 23 is rejected applied as above in rejecting Claim 1. Furthermore, Langford teaches and describes a method of detecting unauthorized executable programs resident in a computer system memory, wherein predetermined data includes system memory locations indicative of executable programs in operation (Column 4 lines 1 – 7).

Claim 24 is rejected applied as above in rejecting Claim 1. Furthermore, Langford teaches and describes a method of detecting unauthorized executable programs resident in a computer system memory, wherein predetermined data is hashed in an absolute memory location independent fashion (Column 4 lines 1 – 14 and Column 8 line 58 – Column 9 line 6).

Claim 18 is rejected applied as above in rejecting Claim 17. Furthermore, Langford teaches and describes a method of detecting unauthorized executable programs resident in a computer system memory, comprising the steps of:

e) comparing a computed hash value with the trusted hash value to detect changes to the predetermined data existing in memory within the computer system (Column 3 line 64 – Column 4 line 8 and Column 8 lines 21 – 33).

Claim 3 is rejected applied as above in rejecting Claim 2. Furthermore, Langford teaches and describes a method of detecting unauthorized executable programs resident in a computer system memory, wherein

the authorization data is at least a biometric information sample (Column 6 lines 2 – 5); and

wherein the step of authenticating includes a step of comparing the at least a biometric information sample to a previously stored biometric template (Column 6 lines 2 – 29).

Claim 4 is rejected applied as above in rejecting Claim 1. Furthermore, Langford teaches and describes a method of detecting unauthorized executable programs resident in a computer system memory, comprising the steps of:

when the comparison is indicative of other than an unauthorized executable programs resident in a computer system, providing the requested security data relating to the user (Column 4 lines 26 – 44).

Claim 7 is rejected applied as above in rejecting Claim 6. Furthermore, Langford teaches and describes a method of detecting unauthorized executable programs resident in a computer system memory, wherein the trusted hash is digitally signed (Column 3 lines 31 – 35 and Column 4 lines 1 – 7 and 26 – 44);

Claim 9 is rejected applied as above in rejecting Claim 8. Furthermore, Langford teaches and describes a method of detecting unauthorized executable programs resident in a computer system memory, comprising the steps of:

receiving a request for security data from an application in execution in the computer system (Column 4 lines 1 – 7); and,

when the authenticity of the digitally signed trusted hash value is verified and the comparison is indicative of other than an unauthorized executable programs resident in a computer system, providing the requested security data to the application (Column 8 lines 21 – 48).

Claim 11 is rejected applied as above in rejecting Claim 8. Furthermore, Langford teaches and describes a method of detecting unauthorized executable programs resident in a computer system memory, comprising the step of:

d) when the computed hash value and the trusted hash value are other than indicative of a known secure state, issuing a notification that an unauthorized executable program is detected within the computer system (Column 6 line 68 – Column 7 line 5).

Claim 19 is rejected applied as above in rejecting Claim 18. Furthermore, Langford teaches and describes a method of detecting unauthorized executable programs resident in a computer system memory, comprising the steps of:

f) verifying the authenticity of the digital signature of the trusted hash value (Column 5 lines 24 – 35 and Column 6 lines 30 – 41).

Claim 13 is rejected applied as above in rejecting Claim 7. Furthermore, Langford teaches and describes a method of detecting unauthorized executable programs resident in a computer system memory, comprising the step of transmitting the trusted hash value to a second other computer system in communication with the computer system and retrievably storing the trusted hash value within the second other computer system (Column 4 lines 1 – 7; Column 5 lines 10 – 15 and Column 8 lines 21 – 48).

Claim 10 is rejected applied as above in rejecting Claim 9. Furthermore, Langford teaches and describes a method of detecting unauthorized executable programs resident in a computer system memory, wherein the application and the predetermined hashing process are both executed on the same processor of the computer system (Column 8 lines 21 – 48).

Claim 12 is rejected applied as above in rejecting Claim 11. Furthermore, Langford teaches and describes a method of detecting unauthorized executable programs resident in a computer system memory, comprising the step of:

e) when the computed hash value and the trusted hash value are other than indicative of a known secure state preventing access to the computer system (Column 8 lines 21 – 48).

Claim 20 is rejected applied as above in rejecting Claim 19. Furthermore, Langford teaches and describes a method of detecting unauthorized executable programs resident in a computer system memory, comprising the steps of:

g) when the computed hash value and the trusted hash value are indicative of a same trusted state of a computer system, providing security data from a trusted source to an application in execution on the system (Column 3 lines 5 – 17 and 36 – 44).

Claim 14 is rejected applied as above in rejecting Claim 13. Furthermore, Langford teaches and describes a method of detecting unauthorized executable programs resident in a computer system memory, including the step of transmitting the computed hash value to the second other computer system for comparison with the trusted hash value by a processor of the second other computer system (Column 8 lines 21 – 48).

Claim 21 is rejected applied as above in rejecting Claim 20. Furthermore, Langford teaches and describes a method of detecting unauthorized executable programs resident in a computer system memory, comprising the step of:

h) when the computed hash value and the trusted hash value are other than indicative of a same secure state of the system, notifying a system administrator (Column 6 line 68 – Column 7 line 5).

Claim 15 is rejected applied as above in rejecting Claim 14. Furthermore, Langford teaches and describes a method of detecting unauthorized executable programs resident in a computer system memory, wherein the computed hash value is a value determined in dependence upon the predetermined data existing in memory within the computer system and some time dependent data of the computer system (Column 4 lines 50 – Column 5 line 8).

Claim 16 is rejected applied as above in rejecting Claim 14. Furthermore, Langford teaches and describes a method of detecting unauthorized executable programs resident in a computer system memory, wherein the second other computer system includes a trusted source wherein security data is stored for provision to applications in execution on systems that are known to be secure (Column 3 lines 5 – 17 and 36 – 44).

Conclusion

9. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

10. Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

11. Applicant is urged to consider the references. However, the references should be evaluated by what they suggest to one versed in the art, rather than by their specific disclosure. If applicants are aware of any better prior art than those are cited, they are required to bring the prior art to the attention of the examiner.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
June 18, 2005.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100